IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE

MARCUS GLASCOCK, individually and on behalf of all others similarly situated, Plaintiff, v. **HCA HEALTHCARE, INC.,** Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Marcus Glascock ("Plaintiff") bring this Class Action Complaint, individually and on behalf of all others similarly situated (the "Class Members"), against Defendant HCA Healthcare, Inc. alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiff.

NATURE OF CASE

1. This class action arises out of the recent, targeted cyberattack and data breach of health provider HCA Healthcare, Inc. ("HCA" or "Defendant"), where unauthorized third-party criminals retrieved and exfiltrated personal data of over 11 million individuals from HCA's network (the "Data Breach").

2. Nashville-based HCA is "one of the nation's leading providers of healthcare services comprising 180 hospitals and approximately 2,300 ambulatory sites of care, including surgery centers, freestanding ERs, urgent care centers, and physician clinics, in 20 states and the United Kingdom."[1]

3. According to HCA, in the Data Breach includes personally identifying information

[1] HCA Healthcare Reports Data Security Incident, HCA Healthcare (July 10, 2023), https://hcahealthcare.com/about/privacy-update.dot.

("PII") and protected health information ("PHI") such as patient names, city, state, zip code, email, telephone number, date of birth, and gender, as well as patient service date, location, and next appointment (collectively, "PII" and "PHI" is "Private Information").[2]

4. Despite its vast experience as a healthcare provider, HCA did not protect the personally identifying information ("PII") and protected health information ("PHI," and, collectively with PII, "Private Information") of its patients—the Class Members.[3]

5. HCA maintained Class Members' Private Information in a negligent and/or reckless manner. In particular, the Private Information was maintained on HCA's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to HCA, and HCA was thus on notice that failing to take steps necessary to secure Private Information from those risks left that Private Information in a vulnerable condition.

6. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes, including opening new financial accounts and taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' Private Information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, and giving false information to police

[2] *Id.*

[3] PII and PHI is referred to collectively throughout as "Private Information" and contains information such as names, physical addresses, phone numbers, dates of birth, health insurance account information, Social Security numbers, provider taxpayer identification numbers, and clinical information (e.g., medical history, diagnoses, treatment, dates of service, and provider names).

during an arrest.

7. As a result of the Data Breach, Plaintiff and Class Members face a substantial risk of imminent and certainly impending harm. Plaintiff and Class Members have and will continue to suffer injuries associated with this risk, including but not limited to a loss of time, mitigation expenses, and anxiety over the misuse of their Private Information.

8. Even those Class Members who have yet to experience identity theft have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft and fraud as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of their Private Information, loss of privacy, and/or additional damages as described below.

9. Accordingly, Plaintiff brings this action against HCA seeking redress for HCA's unlawful conduct and asserting claims for: (i) negligence; (ii) negligence per se; (iii) breach of contract; (iv) unjust enrichment; and (iv) bailment. Through these claims, Plaintiff seeks damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including improvements to HCA's data security systems, future annual audits, and adequate credit monitoring services funded by HCA.

THE PARTIES

10. **Plaintiff Marcus Glascock** is a natural person, resident, and citizen of California.

11. In order to obtain medical services from HCA, Mr. Glascock provided HCA with highly-sensitive Private Information—including financial and health information—which was

then stored on HCA's systems.

12. Mr. Glascock recalls receiving Email Notice from Defendant HCA in July 2023, stating that an unknown actor accessed and obtained certain files on the HCA network containing his Private Information ("Notice"). A copy of the Notice is attached hereto as Exhibit A.

13. HCA obtained and continues to maintain the Private Information of Mr. Glascock and owed him a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Mr. Glascock's Private Information was compromised and disclosed as a result of HCA's inadequate data security, which resulted in the Data Breach.

14. As a result of the Data Breach, Mr. Glascock has experienced increased anxiety and emotional distress over the loss of privacy he experienced because of the Data Breach.

15. Further, Mr. Glascock has experienced emotional distress given the increased likelihood of harm he has been exposed to as a result of HCA's wrongdoing. She has suffered imminent and impending injury arising from the substantially-increased likelihood of fraud, identity theft, and misuse of her Private Information being compromised and placed in the hands of third-party criminals.

16. **Defendant HCA Healthcare, Inc.** is a corporation incorporated in Tennessee, with its headquarters in Nashville, Tennessee. HCA's principal place of business is One Park Plaza, Nashville, Tennessee 37203–6527. Defendant is a citizen of the State of Tennessee

JURISDICTION AND VENUE

17. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiff and at least one member of the putative Class, as defined below, are citizens of a different state than HCA, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest

and costs.

18. This Court has general personal jurisdiction over HCA because HCA maintains its personal place of business in Nashville, Tennessee, regularly conduct business in Tennessee, and has sufficient minimum contacts in Tennessee.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because HCA's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

20. Defendant is a Nashville, Tennessee-based company, founded in 1968, which owns and operates 180 hospitals and approximately 2,300 ambulatory sites of care in the 20 U.S. states and the United Kingdom.[4]

21. HCA generates approximately $60.233 billion annual revenue.[5] HCA trades on the New York Stock Exchange under the stock symbol HCA.[6]

22. To obtain healthcare and related clinical laboratory services, patients, like Plaintiff and Class Members, must provide their highly sensitive Private Information to doctors, medical professionals, or HCA directly. As part of its business, HCA then compiles, stores, and maintains the Private Information it receives from patients and healthcare professionals who submit Class Members' treatments for coverage under HCA's services.

[4] HCA Healthcare Reports Data Security Incident, HCA Healthcare (July 10, 2023), https://hcahealthcare.com/about/privacy-update.dot.
[5] HCA Healthcare Reports Fourth Quarter 2022 Results and Provides 2023 Guidance, HCA Healthcare (Jan. 27, 2023), https://investor.hcahealthcare.com/news/news-details/2023/HCA-Healthcare-Reports-Fourth-Quarter-2022-Results-and-Provides-2023-Guidance/default.aspx.
[6] Stock Information, HCA Healthcare, https://investor.hcahealthcare.com/stockinformation/default.aspx (last accessed July 18, 2023).

23. Because of the highly sensitive and personal nature of the information HCA acquires and stores with respect to patients and other individuals, HCA, upon information and belief, promises to, among other things: keep Private Information private; comply with health care industry standards related to data security and Private Information, including the Health Insurance Portability and Accountability Act of 1996, as amended, and its implementing regulations ("HIPAA"); inform consumers of its legal duties and comply with all federal and state laws protecting consumer Private Information; use and release Private Information only for reasons that relate to medical care and treatment; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

24. As a HIPAA-covered business entity, HCA is required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured Private Information as in the case of the Data Breach complained of herein.

25. However, HCA did not maintain adequate security to protect its systems from infiltration by cybercriminals, and it waited nearly two months to publicly disclose the Data Breach.

26. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, HCA assumed legal and equitable duties to Plaintiff and Class Members, and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

27. HCA was in the best position to safeguard the most sensitive information that it obtained from Plaintiff and Class Members. Its unique position enabled it to collect some of the

most sensitive information on Plaintiff and Class Members; accordingly, HCA had a special relationship with Plaintiff and Class Members such that it should have safeguarded that data.

HCA Is a Covered Entity Subject to HIPAA

28. HCA is a HIPAA-covered entity that provides services to patients and healthcare and medical service providers. As a regular and necessary part of its business, HCA collects the highly sensitive Private Information of its patients.

29. As a covered entity, HCA is required under federal and state law to maintain the strictest confidentiality of the patients' Private Information that it acquires, receives, and collects, and HCA is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

30. As a covered entity, HCA is required to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured Private Information as in the case of the Data Breach complained of herein.

31. Due to the nature of HCA's business, which includes providing a range of healthcare and clinical medical services, including storing and maintaining electronic health records, HCA would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, HCA assumed legal and equitable duties to Plaintiff and Class Members, and it knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

33. Plaintiff and Class Members are or were patients whose Private Information, including medical records, HCA maintained, who received health-related or other services from HCA, and/or individuals who directly or indirectly entrusted HCA with their Private Information.

34. Plaintiff and Class Members relied on HCA to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of their Private Information. Plaintiff and Class Members reasonably expected that HCA would safeguard their highly sensitive information and keep that Private Information confidential.

35. As described throughout this Complaint, HCA did not reasonably protect, secure, or store Plaintiff's and Class Members' Private Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information HCA maintained. Predictably, cybercriminals circumvented HCA's security measures, resulting in a significant Data Breach.

The Data Breach and Email Notice

36. According to the Notice Email HCA provided to Plaintiff and Class Member, HCA discovered that Private Information with respect to at least 11 million patients was leaked online to hacker forums,[7] where such details can sell for a lot of money.[8]

[7] HCA Healthcare Reports Data Security Incident, HCA Healthcare (July 10, 2023), https://hcahealthcare.com/about/privacy-update.dot.

[8] *HCA Healthcare Confirms Huge Data Breach: 11 Million Patients Affected*, Trend Micro(July 13, 2023), https://news.trendmicro.com/2023/07/13/hca-healthcare-data-breach.

37. HCA informed Plaintiff and Class Members HCA determined that "a list of certain information with respect to some of its patients was made available by an unknown and unauthorized party on an online forum."[9]

38. The investigation revealed that the files at issue contained certain Private Information, including patients' name, place of residence, contact information, date of birth, gender, and the patient' service date, location, and next appointment date.[10] According to HCA's disclosure, the Data Breach impacted 27 million rows of data affecting approximately 11 million HCA patients.[11]

39. According to HCA, Plaintiff's and Class Members' Private Information was exfiltrated and stolen in the attack.

40. In the aftermath of the Data Breach, HCA reportedly "disabled user access to the storage location" and plans to engage in "ongoing education for our colleagues, physicians, vendors, and others to maintain awareness of safe practices that can help ensure compliance and the security of our information."[12] In other words, Defendant admits additional security efforts were required, but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' Private Information going forward.

41. In the Email Notice Defendant recommended that Plaintiff and Class Members "remain vigilant about any suspicious or unexpected communications from an unfamiliar source or from anyone claiming to be affiliated with HCA Healthcare," and provides a telephone number

[9] HCA Healthcare Reports Data Security Incident, HCA Healthcare (July 10, 2023), https://hcahealthcare.com/about/privacy-update.dot.
[10] *Id.*
[11] *Id.*
[12] *Id.*

for affected individuals to call if they have any questions or "receive any communication regarding an invoice, outstanding balance, or payment reminder that you were not expecting or believe to be fraudulent" so that HCA "can confirm the legitimacy of the message."[13] However, HCA offers no credit monitoring or identity theft services to the majority of the roughly 11 million affected individuals.[14] Although on its website, HCA claims to "offer credit monitoring and identity protection services, where appropriate," HCA gives no indication as to how it is determining the propriety of that offering, or of the scope or duration of those services when they are offered.[15]

42. HCA's accessed systems contained Private Information that was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor.

43. As HIPAA-covered business entities that collect, create, and maintain significant volumes of Private Information, HCA was aware that a targeted attack was a foreseeable risk that it had a duty to guard against. This is particularly true because the targeted attack appears to have been a ransomware attack. It is well-known that healthcare businesses and insurers such as HCA, which collect and store the confidential and sensitive Private Information of millions of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

44. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients,

[13] Plaintiff's Email Notice of HCA Data Breach, attached as Ex. A.
[14] *Id.*
[15] HCA Healthcare Reports Data Security Incident, HCA Healthcare (July 10, 2023), https://hcahealthcare.com/about/privacy-update.dot.

like Plaintiff and Class Members.

45. HCA had obligations created by HIPAA, contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

46. Plaintiff and Class Members provided their Private Information to HCA with the reasonable expectation and mutual understanding that HCA would comply with its obligations to keep such information confidential and secure from unauthorized access.

47. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, HCA assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

48. Due to HCA's inadequate security measures and its delayed notice to victims, Plaintiff and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

The Data Breach was a Foreseeable Risk of which HCA was on Notice

49. As covered entities handling the medical patient data of insureds, HCA's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry, and other industries holding significant amounts of PII and PHI, preceding the date of the breach.

50. At all relevant times, HCA knew, or should have known that Plaintiff's and Class Members' Private Information was a target for malicious actors. Despite such knowledge, HCA failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' Private Information from cyberattacks that HCA

should have anticipated and guarded against.

51. Considering recent high profile data breaches at other health care providers, HCA knew or should have known that its electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

52. Cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company, Protenus, found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[16]

53. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[17]

54. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000

[16] *2022 Breach Barometer*, PROTENUS, https://blog.protenus.com/key-takeaways-from-the-2022-breach-barometer (2022).
[17] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available at: https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

patients, April 2020), BJC Health System (286,876 patients, March 2020), and Premera Blue Cross (10.4 million patients, January 2015) HCA knew or should have known that its electronic records would be targeted by cybercriminals.

55. Indeed, cyberattacks against the healthcare industry have been common for over eleven years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[18]

56. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[19] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[20] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident in 2010, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[21]

57. Cyberattacks on medical systems, like HCA's, have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities

[18] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.
[19] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (stating "Health information is a treasure trove for criminals.").
[20] *Id.*
[21] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.

and hospitals are attractive . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[22]

58. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents." [23]

59. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[24] In this case, HCA stored the records of *millions* of patients.

60. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[25]

61. Private Information, like that stolen from HCA, is "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web

---

[22] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.
[23] The HIPAA Journal, *Editorial: Why Do Criminals Target Medical Records* (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records.
[24] *See id.*
[25] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[26]

62. Cybercriminals also maintain encrypted information on individuals to sell in "fullz" records because that information can be foreseeably decrypted in the future.

63. HCA was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[27]

64. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[28]

65. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiff

---

[26] *See id.*

[27] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820.

[28] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED.ASS'N (Oct 4, 2019), https://www.ama-assn.org/practice-anagement/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

and Class Members.

66. The U.S. Department of Health and Human Services and the Office of Consumer Rights urges the use of encryption of data containing sensitive personal information. As far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR's deputy director of health information privacy, stated that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[29]

67. As a HIPAA-covered entities, HCA should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in its unprotected files.

HCA Fail to Comply with FTC Guidelines

68. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

69. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct

[29] Susan D. Hall, *OCR levies $2 million in HIPAA fines for stolen laptops*, Fierce Healthcare (Apr. 23, 2014), https://www.fiercehealthcare.com/it/ocr-levies-2-million-hipaa-fines-for-stolen-laptops.

any security problems.[30] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[31]

70. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

71. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

72. These FTC enforcement actions include actions against healthcare providers and partners like HCA. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

[30] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[31] *Id*.

73. HCA failed to properly implement basic data security practices.

74. HCA's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

75. HCA was at all times fully aware of its obligations to protect the Private Information of customers and patients. HCA was also aware of the significant repercussions that would result from its failure to do so.

HCA Fail to Comply with Industry Standards

76. As shown above, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

77. Experts have identified several best practices that at a minimum should be implemented by healthcare service providers like HCA, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

78. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and, training staff regarding critical points.

79. On information and belief, HCA failed to meet the minimum standards of any of

the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

80. These foregoing frameworks are existing and applicable standards in the healthcare industry, and HCA failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

HCA's Conduct Violates HIPAA Obligations to Safeguard Private Information

81. As a healthcare company, and by handing medical patient data, HCA is a covered entity under HIPAA (45 C.F.R. § 160.103) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

82. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

83. HCA is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[5] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

84. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

85. HIPAA-covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

86. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data HCA left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

87. A data breach like the one HCA experienced is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40

88. The Data Breach resulted from a combination of insufficiencies that demonstrate HCA failed to comply with safeguards mandated by HIPAA regulations.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

89. Cyberattacks and data breaches at health care companies like HCA are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

90. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the

attack.[32]

91. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[33]

92. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[34]

93. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims and to take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking

[32] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[33] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019), *available at* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[34] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf.

whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

94. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[35]

95. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

96. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.

97. Moreover, theft of Private Information is also gravely serious because Private

[35] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited May 7, 2023).

Information is an extremely valuable property right.[36]

98. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

99. In addition, there may be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

100. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

101. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

102. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff

[36] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

and Class Members are at an increased risk of fraud and identity theft for many years into the future.

103. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come—as HCA have suggested that they do.

104. Private Information can sell for as much as $363 per record according to the Infosec Institute.[37] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information (and the resulting damage to victims) may continue for years.

105. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[38] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[39] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

106. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

---

[37] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market.
[38] *Identity Theft and Your Social Security Number*, Social Security Administration (July 2021), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf.
[39] *Id*.

107. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[40]

108. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[41]

109. Medical information is especially valuable to identity thieves.

110. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[42]

111. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

112. For this reason, HCA knew or should have known about these dangers and strengthened its data and email handling systems accordingly. HCA was on notice of the

[40] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.
[41] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.
[42] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

substantial and foreseeable risk of harm from a data breach, yet HCA failed to properly prepare for that risk.

HCA Breached its Obligations to Plaintiff and Class Members

113. HCA breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. HCA's unlawful conduct includes, but is not limited to, the following acts and/or omissions based upon information and belief:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect insureds' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out its functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a

confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

p. Failing to adhere to industry standards for cybersecurity as discussed above; and

q. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

114. HCA negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems, which contained Private Information, for multiple weeks.

115. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with HCA for health insurance services.

Plaintiff's and Class Members' Damages

116. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiff and Class Members have all suffered damages and will face a substantial risk of additional injuries for years to come, if not the rest of their lives. Beyond providing inadequate credit monitoring, HCA have done nothing to compensate Plaintiff or Class Members for many of the injuries they have already suffered. HCA have not demonstrated any efforts to prevent additional harm from befalling Plaintiff and Class Members as a result of the Data Breach.

117. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

118. Plaintiff's and Class Members' Private Information was all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed HCA's computer systems.

119. Since being notified of the Data Breach, Plaintiff have spent time dealing with the impact of the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

120. Due to the Data Breach, Plaintiff anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords and monitoring accounts for fraudulent activity.

121. Plaintiff's and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

122. As a direct and proximate result of HCA's conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

123. As a direct and proximate result of HCA's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

124. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

125. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on Plaintiff's and Class Members' Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

126. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, and similar costs directly or indirectly related to the Data Breach.

127. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach.

128. Plaintiff and Class Members were also damaged insofar as they did not receive the benefit of their bargain with HCA. Plaintiff and Class Members overpaid for a service—health insurance—that was supposed to come with adequate data security that complied with industry standards but did not. Part of the price Plaintiff and Class Members paid to HCA for health insurance was intended to be used by HCA to fund adequate security of computer system(s) and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and Class Members did not get what they paid for and agreed to.

129. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

130. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare

providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

131. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of HCA, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

132. Further, as a result of HCA's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

133. As a direct and proximate result of HCA's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

134. Plaintiff brings this action against HCA individually and on behalf of all other persons similarly situated ("the Classes").

135. Plaintiff proposes the following Class definition (the "Nationwide Class"), subject to amendment as appropriate:

> **All persons or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, who HCA identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Nationwide Class").**

136. Plaintiff also proposes to represent a state subclass, defined as follows and subject to amendment as appropriate:

> **All California residents or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, who HCA identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "California Subclass").**

137. Excluded from the Classes are HCA's officers, directors, and employees; any entity in which HCA have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of HCA. Excluded also from the Classes are members of the judiciary to whom this case is assigned, their families and Members of their staff.

138. Plaintiff reserves the right to amend or modify the Class definitions or create additional subclasses as this case progresses.

139. ***Numerosity***. The Members of the Classes are so numerous that joinder of all of them is impracticable. HCA disclosed that over 11 million Class Members had their Private Information compromised in Data Breach.

140. ***Commonality***. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether HCA unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether HCA failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether HCA's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;

d. Whether HCA's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether HCA owed a duty to Class Members to safeguard their Private Information;

f. Whether HCA breached their duty to Class Members to safeguard their Private Information;

g. Whether HCA knew or should have known that their data security systems and monitoring processes were deficient;

h. Whether HCA should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of HCA's misconduct;

j. Whether HCA's conduct was negligent;

k. Whether HCA breached implied contracts with Plaintiff and Class Members;

l. Whether HCA was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. Whether HCA failed to provide notice of the Data Breach in a timely

manner, and;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

141. ***Typicality***. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

142. ***Adequacy of Representation***. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

143. ***Predominance***. HCA have engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and Class Members' Private Information was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from HCA's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

144. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would also create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for HCA. In contrast, to conduct this action as a class action presents far fewer management difficulties,

conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

145. ***Declaratory and Injunctive Relief Appropriate.*** HCA has acted on grounds that apply generally to the Classes as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

146. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether HCA failed to timely notify the public of the Data Breach;

b. Whether HCA owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether HCA's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether HCA's failure to institute adequate protective security measures amounted to negligence;

e. Whether HCA failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

147. Finally, all members of the proposed Classes are readily ascertainable. HCA has

access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by HCA.

CLAIMS FOR RELIEF

COUNT I
Negligence
(*On Behalf of Plaintiff and the Nationwide Class*)

148. Plaintiff re-alleges and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

149. By collecting and storing the Private Information of Plaintiff and Class Members, in its computer system and network, and sharing that Private Information and using it for commercial gain, HCA owed a duty of care to use reasonable means to secure and safeguard their computer system—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. HCA's duties included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious time and to give prompt notice to those affected in the case of a data breach.

150. HCA owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

151. Plaintiff and Class Members are a well-defined, foreseeable, and probable group of patients that HCA was aware, or should have been aware, could be injured by inadequate data security measures.

152. HCA's duty of care to use reasonable security measures arose as a result of the

special relationship that existed between HCA and insured consumers, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. HCA was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

153. HCA's duty to use reasonable security measures under HIPAA required HCA to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

154. In addition, HCA had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

155. HCA's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because HCA is bound by industry standards to protect confidential Private Information.

156. HCA breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by HCA include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

157. Plaintiff and Class Members have no ability to protect their Private Information that was or remains in HCA's possession.

158. It was foreseeable that HCA's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

159. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members. In addition, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

160. HCA's conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect Class Members' Private Information and failing to provide Plaintiff and Class Members with timely notice that their Private Information had been compromised.

161. Neither Plaintiff nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

162. Plaintiff and Class Members are also entitled to injunctive relief requiring HCA to, among other things, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring and identity theft protection services to all Class Members.

163. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of HCA's breach of its duties. HCA knew or should have known that it was failing to meet its duties and that HCA's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

164. As a direct and proximate result of HCA's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, nominal, and other damages as appropriate and ordered by the Court in an amount to be proven at trial.

COUNT II
Negligence Per Se
(On behalf of the Plaintiff and the Nationwide Class)

165. Plaintiff re-alleges and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

166. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

167. HCA violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Private Information and not complying with industry

standards. HCA's conduct was particularly unreasonable given the nature and amount Private Information obtained and stored and the foreseeable consequences of a data breach on HCA's systems.

168. HCA also violated HIPAA and HIPPA privacy rules and regulations. A data breach like the one HCA experienced is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule.

169. HCA's violations of HIPAA, Section 5 of the FTC Act and analogous provisions of Tennessee law constitute negligence *per se*.

170. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) and HIPAA were intended to protect.

171. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) and HIPAA was intended to guard against. Indeed, the FTC has pursued enforcement actions against businesses which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

172. As a direct and proximate result of the HCA's negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such damages include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the compromised Private Information; illegal sale of the compromised Private Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and

unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their Private Information; lost value of unauthorized access to their Private Information; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT III
Breach of Implied Contract
(On behalf of the Plaintiff and the Nationwide Class)

173. Plaintiff re-alleges and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

174. HCA acquired and maintained the Private Information of Plaintiff and the Class that it received either directly or from its healthcare provider customers.

175. When Plaintiff and Class Members paid money and provided their Private Information to their doctors and/or healthcare providers, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with their doctors and/or healthcare professionals, their business associates, and pharmacies, including HCA.

176. Plaintiff and Class Members entered into implied contracts with HCA under which HCA agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

177. Plaintiff and the Class were required to deliver their Private Information to HCA as part of the process of obtaining services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

178. HCA solicited, offered, and invited Plaintiff and Class Members to provide their Private Information as part of HCA's regular business practices. Plaintiff and Class Members

accepted HCA's offers and provided their Private Information to HCA, or, alternatively, provided Plaintiff's and Class Members' information to doctors or other healthcare professionals, who then provided to HCA.

179. HCA accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services or Plaintiff and Class Members.

180. In accepting such information and payment for services, HCA entered into an implied contract with Plaintiff and the other Class Members whereby HCA became obligated to reasonably safeguard Plaintiff's and the other Class Members' Private Information.

181. Alternatively, Plaintiff and Class Members were the intended beneficiaries of data protection agreements entered into between HCA and healthcare providers.

182. In delivering their Private Information to HCA and paying for healthcare services, Plaintiff and Class Members intended and understood that HCA would adequately safeguard the data as part of that service.

183. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

184. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6)

multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

185. Plaintiff and the Class Members would not have entrusted their Private Information to HCA in the absence of such an implied contract.

186. Had HCA disclosed to Plaintiff and the Class (or their physicians) that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members would not have provided their Private Information to HCA (or to their physicians to provide to HCA).

187. HCA recognized that Plaintiff's and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

188. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with HCA.

189. HCA breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

190. As a direct and proximate result of HCA's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

191. Plaintiff re-alleges and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

192. This count is pleaded in the alternative to any breach of contract claim.

193. Upon information and belief, HCA funds its data security measures entirely from

general revenue, including from money it makes based upon protecting Plaintiff's and Class Members' Private Information.

194. There is a direct nexus between money paid to HCA and the requirement that HCA keep Plaintiff's and Class Members' Private Information confidential and protected.

195. Plaintiff and Class Members paid HCA and/or healthcare providers a certain sum of money, which was used to fund data security via contracts with HCA.

196. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members was to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to HCA.

197. Protecting Plaintiff's and the rest of the Class Members' Private Information is integral to HCA's business. Without Class Members' data, neither Defendant would be able to provide insurance services, thus comprising each Defendant's core business.

198. Plaintiff's and Class Members' Private Information has monetary value, and Plaintiff and Class Members directly and indirectly conferred a monetary benefit on each Defendant. They indirectly conferred a monetary benefit on each Defendant by purchasing goods and/or services from entities that contracted with each Defendant, and from which each Defendant received compensation to protect certain data. Plaintiff and Class Members directly conferred a monetary benefit on HCA, both directly and by supplying Private Information, which has value, from which value HCA derives its business value, and which should have been protected with adequate data security.

199. HCA knew that Plaintiff and Class Members conferred a benefit that HCA accepted. HCA profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

200. HCA enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, HCA instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of HCA's failure to provide the requisite security.

201. Under the principles of equity and good conscience, HCA should not be permitted to retain the money belonging to Plaintiff and Class Members because HCA failed to implement appropriate data management and security measures that are mandated by industry standards.

202. HCA acquired the monetary benefit and Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

203. If Plaintiff and Class Members knew that HCA had not secured their Private Information, they would not have agreed to provide their Private Information to HCA.

204. Plaintiff and Class Members have no adequate remedy at law.

205. As a direct and proximate result of HCA's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the

Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in HCA's possession and is subject to further unauthorized disclosures so long as HCA fail to undertake appropriate and adequate measures to protect Private Information in its possession; (vii) loss or privacy from the authorized access and exfiltration of their Private Information; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

206. As a direct and proximate result of HCA's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

207. HCA should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, HCA should be compelled to refund the amounts that Plaintiff and Class Members overpaid for HCA's services.

COUNT V
Bailment
(*On Behalf of Plaintiff and the Nationwide Class*)

208. Plaintiff re-alleges and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

209. Plaintiff and Class Members provided Private Information to the HCA—either directly or through healthcare providers and their business associates—which HCA was under a duty to keep private and confidential.

210. Plaintiff's and Class Members' Private Information is personal property, and it was conveyed to HCA for the certain purpose of keeping the information private and

confidential.

211. Plaintiff's and Class Members' Private Information has value and is highly prized by hackers and criminals. HCA was aware of the risks it took when accepting the Private Information for safeguarding, and it assumed the risk voluntarily.

212. Once HCA accepted Plaintiff's and Class Members' Private Information, neither Plaintiff nor Class Members could control that information.

213. HCA did not safeguard Plaintiff's or Class Members' Private Information when it failed to adopt and enforce adequate security safeguards to prevent a known risk of a cyberattack.

214. HCA's failure to safeguard Plaintiff's and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

215. As a result of HCA's failure to keep Plaintiff's and Class Members' Private Information secure, Plaintiff and Class Members suffered injury, for which compensation—including nominal damages and compensatory damages—are appropriate.

COUNT VI
Deceptive Trade Practices
Tenn. Code Ann. § 47-18-104
(*On Behalf of Plaintiff and the Nationwide Class*)

216. Plaintiff re-alleges and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

217. Defendant violated Tenn. Code Ann. § 47-18-104 by engaging in deceptive acts or practices in the conduct of its business and the furnishing of its services in the State of Tennessee.

218. Defendant's deceptive practices include omitting, suppressing, and concealing the material fact that it did not have and did not reasonably ensure that it reasonably or adequately

secured Plaintiff's and Class Members' Personal Information.

219. Defendant engaged in acts of deception and false pretense in connection with its accepting, collecting, securing, and otherwise protecting patient Personal Information and engaged in the following deceptive trade practices, including:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class Members' Personal Information;

b. Failing to comply with data security standards during the period of the Data Breach;

c. Failing to comply with regulations protecting the Personal Information at issue during the period of the Data Breach;

d. Failing to adequately monitor, evaluate, and ensure the security of its network and systems;

e. Failing to recognize in a timely manner that Plaintiff's and other Class Members' Personal Information had been compromised; and

f. Failing to timely and adequately disclose that Plaintiff's and Class Members' Personal Information had been improperly acquired or accessed.

220. Plaintiff's and Class Members' Personal Information would not have been compromised but for Defendant's wrongful and unfair breach of its duties.

221. Defendant's failure to take proper security measures to protect sensitive Personal Information of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class Members' Personal Information.

222. Plaintiff and Class Members conferred a benefit on Defendant—payment for medical services—in reliance on Defendant's omissions and deceptive practices. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not adequately secure patients' Personal Information, Plaintiff and Class Members would not have sought or purchased services from Defendant.

223. As a direct and proximate result of Defendant's fraudulent acts and practices, Plaintiff and Class Members were injured and lost money or property, and monetary and nonmonetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein.

224. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's fraudulent business practices or use of their Personal Information; reasonable attorneys' fees and costs under Tenn. Code Ann. § 47-18-109; injunctive relief; and other appropriate equitable relief.

COUNT VII
Violation of the California Confidentiality of Medical Information Act ("CMIA")
Cal. Civ. Code §§ 56, *et seq*.
(On Behalf of Plaintiff and the California Subclass)

225. Plaintiff re-alleges and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

226. Plaintiff brings this claim on his own behalf and on behalf of the California Subclass.

227. California's Confidential Medical Information Act was enacted to protect, among other things, the release of confidential medical information without proper authorization. See

Confidential Medical Information Act, Cal. Civ. Code §§ 56, et seq. ("CMIA"). To that end, the CMIA prohibits entities from negligently disclosing or releasing any person's confidential medical information. See Cal. Civ. Code § 56.36 (2013).

228. The CMIA also requires that an entity, such as Defendant, that "creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein." Civ. Code § 56.101(a).

229. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

230. Defendant is a "provider of healthcare" within the meaning of Civil Code § 56.05 and .06, and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients" of Defendant, within the meaning of Civil Code § 56.05(k).

231. Plaintiff and California Subclass members are "patients" within the meaning of Civil Code § 56.05(k) and are "endanger[ed]" within the meaning of Civil Code § 56.05(e) because Plaintiff and California Subclass members fear that disclosure of their medical information could subject them to harassment or abuse.

232. Plaintiff and California Subclass members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network at the time of the breach.

233. Defendant, through inadequate security, allowed unauthorized third-party access to Plaintiff's and California Subclass members' medical information, without the prior written authorization of Plaintiff and California Subclass members, as required by Civil Code § 56.10 of

the CMIA.

234. In violation of Civil Code § 56.10(a), Defendant disclosed Plaintiff's and California Subclass members' medical information without first obtaining an authorization. Plaintiff's and California Subclass members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.10(a).

235. In violation of Civil Code § 56.10(e), Defendant further disclosed Plaintiff's and California Subclass members' medical information to persons or entities not engaged in providing direct health care services to Plaintiff or California Subclass members, or to their providers of health care or health care service plans or their insurers or self-insured employers.

236. HCA violated Civil Code § 56.101 of the CMIA through its willful and knowing failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the California Subclass. Defendant's conduct with respect to the disclosure of confidential medical information was willful and knowing because Defendant designed and implemented the computer network and security practices that gave rise to the Data Breach.

237. In violation of Civil Code § 56.101(a), Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and California Subclass members' medical information in a manner that failed to preserve and breached the confidentiality of the information contained therein. Plaintiff's and California Subclass members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

238. In violation of Civil Code § 56.101(a), Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and California Subclass members' medical information. Plaintiff's and California Subclass members' medical information

was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

239. Plaintiff's and California Subclass members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

240. In violation of Civil Code § 56.101(b)(1)(A), Defendant's electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information. Plaintiff's and California Subclass members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(b)(1)(A).

241. Defendant violated Civil Code § 56.36 of the CMIA through its failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the California Subclass.

242. As a result of Defendant's above-described conduct, Plaintiff and California Subclass members have suffered damages from the unauthorized disclosure and release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101, 56.36.

243. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and California Subclass members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of

their PII/PHI, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

244. Plaintiff, individually and for each member of the California Subclass, seeks nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to $3,000 per Plaintiff and each California Subclass member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

COUNT VIII
California Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq*.
(*On Behalf of Plaintiff and the California Subclass*)

245. Plaintiff re-allegess and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

246. Plaintiff brings this claim on their own behalf and on behalf of the California Subclass.

247. Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

248. Defendant violated Cal. Bus. & Prof. Code § 17200 et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

249. Defendant's "unfair" acts and practices include:

a. Defendant failed to implement and maintain reasonable security measures to protect Plaintiff's and California subclass members' Private Information

from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Defendant data breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. Defendant' failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 et seq.), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. Defendant's failure to implement and maintain reasonable security measures also led to substantial injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant' inadequate security, consumers could not have reasonably avoided the harms that Defendant caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

250. Defendant as engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumer

Privacy Act, Cal. Civ. Code § 1798.150, California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C.§ 45, and California common law.

251. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California subclass members' personal information, which was a direct and proximate cause of the Defendant data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Defendant's data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 et seq., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, which was a direct and proximate cause of the Defendant's data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California subclass members' personal information, including duties imposed by the

FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California subclass members' personal information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150.

252. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' personal information.

253. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California subclass members were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, suffered monetary damages from fraud and identity theft, incurred time and expenses related to monitoring their financial accounts for fraudulent activity, are at an increased, imminent risk of fraud and identity theft, and suffered a loss of value of their personal information.

254. Defendant's violations were, and are, willful, deceptive, unfair, and

unconscionable.

255. Plaintiff and California subclass members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

256. By deceptively storing, collecting, and disclosing their personal information, Defendant has taken money or property from Plaintiff and class members.

257. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California subclass members' rights. Past data breaches put it on notice that its security and privacy protections were inadequate.

258. Plaintiff and California subclass members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and his counsel as Class Counsel;

b) For equitable relief enjoining HCA from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling HCA to utilize appropriate methods and policies

with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of HCA's wrongful conduct;

e) Ordering HCA to pay for not less than five years of credit monitoring and identity theft protection services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, nominal damages, statutory penalties, and other damages the Court deems appropriate, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) Pre- and post-judgment interest on any amounts awarded; and,

i) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: August 7, 2023

Respectfully Submitted,

Kim D. Stephens, P.S., WSBA #11984*
Cecily C. Jordan, WSBA #50061*
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Tel: (206) 682-5600/Fax: (206) 682-2992
kstephens@tousley.com
cjordan@tousley.com

Mark P. Chalos
mchalos@lchb.com
Kenneth S. Byrd
kbyrd@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
222 2nd Ave S #1640
Nashville, TN 37201
Tel: 615-313-9000

Jason L. Lichtman*
jlichtman@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLC
250 Hudson Street, 8th Floor
New York, NY 10013-1314
Tel: 212-355-9500

Michael W. Sobol*
msobol@lchb.com
Jallé H. Dafa*
jdafa@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLC
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Tel: 415-956-1000

** Pro Hac Vice Forthcoming*

Counsel for Plaintiff and the Proposed Class

EXHIBIT A

[redacted]

From: HCA Healthcare <noreply@hcahealthcare.com>
Date: July 16, 2023 at 6:24:39 AM PDT
To: [redacted]
Subject: HCA Healthcare Privacy Incident

On Monday, July 10, 2023, we announced that a list of certain information with respect to some of our patients was made available by an unknown and unauthorized party on an online forum. The list includes:

- patient name, city, state, and zip code;
- patient email, telephone number, date of birth, gender; and
- patient service date, location and next appointment date.

Importantly, the list **does not include:**

- clinical information, such as treatment, diagnosis, or condition;
- payment information, such as credit card or account numbers;
- sensitive information, such as passwords, driver's license or social security numbers.

Additional information about the data security incident can be found at hcahealthcare.com/privacyupdate.

We remain committed to protecting the personal information that is entrusted to us. Because patient contact information was involved in this incident, we encourage you to remain vigilant about any suspicious or unexpected communications from an unfamiliar source or from anyone claiming

to be affiliated with HCA Healthcare. **You can call us at 888-993-0010.** Representatives will be available to provide assistance Monday through Friday, 8 am – 8 pm Central Time beginning Monday, July 17. Specifically, if you receive any communication regarding an invoice, outstanding balance, or payment reminder that you were not expecting or believe to be fraudulent, please contact us so that we can confirm the legitimacy of the message.

We are working as quickly as possible to identify and contact patients whose data was impacted by this data security incident. Those individuals can expect to receive a mailed notification letter in the coming weeks and will be offered complimentary credit monitoring and identity protection services.

We appreciate your patience as we continue to work through this event.

Sincerely,
Kathi Whalen
SVP and Chief Ethics and Compliance Officer
HCA Healthcare